

Você está
preparado
para a
LGPD?



APROVEITE AS FUNÇÕES INTERATIVAS DESSE EBOOK!

Esse PDF interativo possibilita links, botões e um índice clicável, assim você pode fazer sua leitura com muito mais praticidade e agilidade.

No canto superior esquerdo, em todas as páginas, você encontrará botões para as nossas redes sociais.

Na parte inferior de cada página, verá um botão que automaticamente retorna ao Índice.

No índice clicável, você pode ir diretamente para o capítulo que deseja.

Por fim, sempre que o texto estiver [assim](#), significa que é um link para uma página externa, para que você possa se aprofundar em algumas informações!

Esperamos que essas funções te ajudem na leitura do texto.

VOCÊ ESTÁ PREPARADO PARA A LGPD?

Dados são o novo petróleo. Essa máxima, repetida tantas vezes em meios tecnológicos e jurídicos, reflete a importância de um bem estratégico e valioso: a informação.

Ao passo que a internet evoluiu, e junto com ela os negócios que nasceram neste novo formato e que usam dados como matéria-prima, agentes internacionais se mobilizaram para medir os impactos do uso indevido de informações pessoais e para pensar formas de proteger os dados e regularizar seu uso perante a lei. Como consequência, foi criada a lei

General Data Protection Regulation (GDPR), na União Europeia. A legislação incide sobre quais dados podem ser de acesso comercial, como as empresas devem tratá-los e, ainda, instituiu regras para a proteção à privacidade deles.

Seguindo a tendência mundial, em agosto de 2018 o governo brasileiro sancionou uma lei que regula a captação e tratamento de dados pessoais no País. A Lei Geral de Proteção de Dados - [Lei 13.709/18](#), ou LGPD, como ficou conhecida, dispõe sobre o tratamento de dados pessoais, tanto no âmbito online como offline, e estabelece dez bases legais para a coleta e o processamento de dados. Além disso, busca estabelecer regras e princípios gerais para que estas possam ser cumpridas de maneira mais benéfica aos titulares dos dados.

Neste e-book, falaremos sobre ambas legislações, como elas impactam no setor de mídia programática e de que forma sua empresa pode estar em *compliance* com a lei. Acompanhe.

ÍNDICE

01.	Entenda as Leis	05
02.	Impacto da LGPD na mídia programática	09
03.	Como se preparar para a LGPD	12
04.	Recapitulando: Check list para estar em compliance com a lei	17
05.	Atualize-se	19

ENTENDA AS LEIS



GDPR

O conjunto de normas que regula o uso de dados pessoais provenientes de pessoas naturais localizadas na União Europeia, entrou em vigor no dia 25 de maio de 2018. A lei foi a primeira a dar um passo no sentido de regular como as empresas poderiam se apropriar de informações alheias.

Com foco na proteção dos direitos dos titulares dos dados e no livre fluxo informacional, a GDPR legisla a favor dos direitos dos usuários da internet na União Europeia. Ao mesmo tempo, ela também se aplica a todas as empresas de diferentes países que fornecem serviços ou produtos e/ou coletam dados relativos ao perfil comportamental de pessoas naturais, sejam elas moradoras ou que estejam em trânsito naquele continente.

De forma resumida, as diretrizes da lei impõem que as empresas tenham posse somente dos dados estritamente necessários para suas operações e que o titular dos dados tenha controle sobre o que ele quer ou não fornecer. Os principais pontos da regulamentação são:

- 01.** Explicitar a autorização do usuário para o compartilhamento e uso de seus dados pela empresa;
- 02.** Evidenciar para o usuário de determinado serviço ou produto online quais dados exatamentes serão armazenados, para que fim estes serão usados e como será feito seu processamento. Por demais, as empresas ainda terão que tipificar as consequências possíveis em caso de não autorização do uso das informações;
- 03.** Explicitar o tempo em que a empresa terá posse dos dados ou como é determinado este intervalo;
- 04.** Particularizar se a informação é proveniente de fonte pública ou se foi solicitada diretamente do usuário; e

05. Permitir que o usuário possa acessar, retificar, apagar ou retirar o consentimento do uso de seus dados a qualquer instante.

Naturalmente, as empresas mais impactadas pela GDPR são as que atuam em áreas como tecnologia e marketing, que dependem das informações para executar seus modelos de negócio. Se em conformidade com a lei, a regulamentação não deve impor nenhum impasse para o funcionamento destas empresas.

Caso a lei seja descumprida em qualquer nível, as sanções variam em multas de até 4% da receita anual da empresa desregular ou 20 milhões de euros, o montante que for maior. O Google, por exemplo, foi multado em **USD 57 milhões**, na França, por não ser claro com os usuários do País na questão que tange privacidade e segurança de dados.

LGPD

A correspondente brasileira da Lei foi sancionada pouco depois do anúncio da legislação europeia. A demanda por regras mais claras quanto a regulação das empresas que atuam com dados no Brasil é antiga. Em 2014, em específico, entrou em vigor o [Marco Civil da Internet](#), que legisla sobre os deveres, obrigações, princípios e garantias de quem usa a internet no País, bem como as diretrizes de atuação do Estado em caso de desrespeito ao acordado.

Em 14 de agosto de 2018 foi sancionada a Lei 13.709/18, denominada [Lei Geral de Proteção de Dados \(LGPD\)](#), que altera o Marco Civil da Internet e cria uma regulamentação para o uso, proteção e transferência de dados pessoais no Brasil, além de estabelecer quem são as figuras envolvidas e suas responsabilidades.

A LGPD estabelece bases legais para justificar o tratamento de dados pessoais, por meio da enumeração de 10 hipóteses, são elas:

- 01.** O consentimento do titular;
- 02.** O cumprimento de obrigação legal ou regulatória pelo controlador;
- 03.** A execução de Políticas Públicas;
- 04.** A realização de estudos por órgãos de pesquisa;
- 05.** A execução de contrato de qual seja parte o titular;
- 06.** O exercício regular de direito em processo judicial, administrativo ou arbitral;
- 07.** A proteção à vida;

- 08.** A tutela da saúde;
- 09.** O legítimo interesse; e
- 10.** A proteção ao crédito.

Caso haja descumprimento da normativa e suas hipóteses de uso de dados, as empresas poderão ser advertidas, multadas ou proibidas de continuar exercendo o tratamento de dados. A multa pode ter o custo de até 2% do faturamento da empresa, sendo limitada em R\$ 50 milhões por infração. As empresas brasileiras, ou as que atuam no território nacional, têm até agosto de 2020 para se adequar às novas regras.



IMPACTO DA LGPD NA MÍDIA PROGRAMÁTICA



O marketing digital é, em sua maioria, baseado em dados pessoais como forma de segmentar as campanhas e atingir um público que faça sentido para as marcas. Com as mudanças na regulamentação do tratamento destas informações, algumas práticas precisarão de adaptações.

Para fim de regulamentação, dados pessoais são especificados como informações que podem tornar um indivíduo identificado ou identificável, como por exemplo: nome, RG, CPF, profissão e outros. Em *compliance* com a lei, as empresas terão que ser mais transparentes e explicar para o titular de dados para que fim serão utilizados estes dados, tendo este a opção de conceder ou não uma hipótese autorizativa para essa coleta. Além disso, será preciso adequar a captação de dados apenas para as finalidades de legítimo interesse das empresas, garantir a segurança dos mesmos e expor ao titular como suas informações estão sendo usadas e protegidas.

A regulamentação aumenta as obrigações dos publishers e anunciantes em informar aos usuários como seus dados serão utilizados. Portanto, as empresas que participam do ecossistema de publicidade online terão que controlar melhor o acesso aos dados coletados e ser transparentes com os usuários quanto ao tratamento e processamento de suas informações.

Toda a cadeia de [mídia programática](#) terá que se adequar à legislação. Os *publishers* que quiserem usar dados para fornecer conteúdo ou anúncios personalizados para sua audiência precisarão usar a base legal apropriada e fornecer transparência às empresas que desejam rastreá-lo. É preciso garantir que todas as diretrizes da lei, elencadas anteriormente, estejam sendo cumpridas. Além do consentimento, que é o primeiro passo para a regulamentação, os *publishers* precisam estar atentos a questões como necessidade, adequação, garantia da integridade dos dados, segurança e todas as hipóteses levantadas pela lei.



As empresas de publicidade que consomem dados provenientes de data centers ou DMPs precisarão ter o cuidado de verificar se seus fornecedores de informação estão também em conformidade com a lei. Para o [onboarding de CRM](#), por exemplo, os dados pessoais precisam primeiro passar por um processo de anonimização para tirar informações identificáveis. Dessa forma é possível traçar perfis e moldar audiências sem infringir a lei.

A nova regra, portanto, altera substancialmente a forma como os profissionais de marketing lidam com os dados. Todos os agentes envolvidos na operação precisarão demonstrar como estão adequados às normativas legais. Para isso, um dos fatores mais importantes é a comprovação da relevância da coleta de dados — quanto mais segmentada para a audiência correta for a campanha, mais ela será relevante para o usuário final.

COMO SE PREPARAR PARA A LGPD



Dias antes da GDPR entrar em vigor, apenas 7% dos entrevistados pela [pesquisa realizada pelo SAS](#), disseram estar totalmente adaptados às novas normas. No Brasil, a realidade não é diferente, mesmo que o prazo para o *compliance* total com a nova normativa seja longo, poucas empresas estão procurando formas de se adaptarem. As que estão caminhando para a conformidade, portanto, apresentam um diferencial competitivo no mercado.

A aprovação da LGPD impôs adequações técnicas para as empresas, mas, além delas, os negócios terão que promover uma adaptação de *mindset* nos seus clientes e colaboradores. Isso porque a norma não abre brechas para pequenos erros, e as consequências financeiras e de reputação destes podem ser determinantes para o futuro da empresa.

Por isso, para ficar em conformidade com a nova regulação, as empresas que atuam no ecossistema *online* de publicidade precisam ir além de notificações de atualização da política de privacidade. É importante ter em mente que somente a adoção de uma política de privacidade não é suficiente. Portanto, é recomendável realizar um DPIA (Data Protection Impact Assessment) ou Relatório de Impacto à Proteção de Dados. Esta metodologia permite, de forma concreta, mapear o fluxo de dados pessoais e processos da empresa, sendo possível, a partir dele, criar um planejamento para estar em conformidade com todas as obrigações legais existentes. Mas este processo não é único, e sim contínuo. Por isso, conduzir periodicamente novas avaliações de proteção de dados e garantir que novos riscos identificados sejam ajustados perante a lei é uma das chaves para o sucesso de um Programa de Privacidade.

Para estar em conformidade com a lei é importante adotar boas práticas, como por exemplo: (i) deixar explícita a finalidade do uso dos dados que estão sendo coletados; (ii) coletar apenas as informações necessárias para a finalidade que se almeja alcançar; (iii) ser transparente nos seus processos de tratamento e captação de dados; (iv) deixar uma opção clara para o titular excluir suas informações que

não quer mais compartilhar; e (v) manter um forte sistema de segurança de dados. Confira as principais ações para se preparar para a LGPD:

Consentimento do usuário:

De acordo com a lei, o consentimento, que é uma das bases legais possíveis, quando utilizado, precisa ser uma “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. A redação exclui a possibilidade dos usuais boxes pré-preenchidos ao fim de termos de uso e privacidade. A partir da entrada em vigor da lei, os responsáveis terão que modificar a forma como a autorização do titular é obtida de modo que os termos presentes nesta estejam claros.

Todos os processos diferentes do que os acordados no primeiro momento que, porventura venham a ser realizados com os dados, necessitam ser previamente informados e autorizados pelo proprietário das informações.

O titular deve, de acordo com a lei, poder revogar o consentimento a qualquer instante de forma simplificada.

Ser claro, transparente e acessível nas informações:

As medidas de proteção de dados devem ser informadas de forma clara, transparente e acessível. O usuário deve poder encontrar e entender como a empresa em si está trabalhando para proteger seus dados. Em caso de invasão e roubo das informações, os detentores são obrigados a informar imediatamente aos titulares afetados, estando estes cientes do que foi feito para evitar o incidente.

As empresas que tratam e processam os dados devem explicitar para qual finalidade estes serão utilizados. A lei estipula que as empresas tenham posse apenas de dados que tenham comprovada utilidade para as mesmas e que

sejam compatíveis com a finalidade dos negócios. Além do mais, por vezes os controladores dos dados terão que provar o legítimo interesse em ter posse e processar tais informações. Por conta disso, ter mais dados do que o estritamente necessário deixa de ser uma vantagem.

Restrição de conteúdo:

Os usuários que não concordarem em disponibilizar seus dados para acessar determinado tipo de conteúdo não podem sofrer restrições, desde que a empresa tenha uma justificativa válida para tanto. Se o titular não der o seu consentimento, quando esta for a base legal aplicável, a empresa deve encontrar um meio de oferecer o serviço ou conteúdo, indicando ao titular que este serviço ou conteúdo poderá sofrer algum tipo de restrição no fornecimento, devido a ausência de alguns dados.

Ferramentas para garantir a privacidade:

É de suma importância ter a convicção de que a operação está em conformidade com a legislação. Para isso, o primeiro objeto de estudo precisa ser a própria empresa. Realizar uma auditoria interna periódica para se certificar de que tudo está de acordo com a norma e corrigir possíveis falhas é essencial para evitar se surpreender com inexatidões — que podem ser passíveis de multa.

A lei aponta a necessidade das empresas indicarem um encarregado de proteção de dados, mais conhecido como Data Protection Officer (DPO). O papel deste encarregado é gerenciar e supervisionar a adoção pela empresa de todas as obrigações legais relativas ao tema de proteção de dados, assim como garantir que todos os processos internos dela cumpram a legislação aplicável ao tema.

Ferramentas que mapeiam o fluxo do uso de dados pessoais também podem ser utilizadas para tanto identificar pontos de atenção, quanto garantir a segurança dos dados que a empresa tem posse.

PLATAFORMAS QUE GARANTEM A PROTEÇÃO DE DADOS

Por mais que grande parte das empresas ainda estejam se familiarizando com as legislações, as plataformas que contam com uma DMP em *compliance* com as novas normas devem adotar alguns pilares que contribuem para garantir o cumprimento da lei:

- **Adequação:** Coletar dados compatíveis com a finalidade dos serviços e com as expectativas dos titulares desses dados;
- **Necessidade:** Coletar apenas os dados necessários para desempenhar os serviços;
- **Transparência:** Fornecer as informações de forma clara e adequada sobre a coleta e tratamento dos dados;
- **Privacy by design:** Criação de um [Privacy Dashboard](#), para que os visitantes, usuários e clientes tenham acesso às suas informações, onde é possível editar ou solicitar a exclusão dos seus dados pessoais;
- **Security by design:** Adotar uma série de medidas de proteção de dados contra acessos não autorizados; e
- **Finalidades:** A finalidade dos dados coletados tem que ser legítima, específica e conhecida do titular dos dados.

RECAPITULANDO: CHECK LIST PARA ESTAR EM *COMPLIANCE* COM A LEI



Por ser extensa e detalhada, a lei, por vezes, se torna de difícil compreensão e cada ponto que não for seguido à risca pode ser passível de sanções. Por isso, preparamos um check list com as principais atitudes que devem ser tomadas para estar em conformidade com a lei dentro do prazo estabelecido:

- 01.** Fazer auditoria interna para garantir a segurança dos dados já em posse da empresa;
- 02.** Captar somente dados compatíveis com o serviço prestado pela empresa;
- 03.** Explicitar a autorização do uso dos dados do usuário com check box sem preenchimento automático;
- 04.** Explicar na mensagem de autorização do uso de dados para qual finalidade exatamente os mesmos serão destinados;
- 05.** Renovar a autorização do uso de dados periodicamente e a cada mudança de função das informações;
- 06.** Contar com parceiros que sejam comprometidos com a regularidade da lei;
- 07.** Não fazer tratamento de dados para fins discriminatórios, ilícitos ou abusivos;
- 08.** Ter um DPO para garantir a adequada governança dos dados da empresa;
- 09.** Encontrar meios de não restringir conteúdos em detrimento da autorização do uso de dados;
- 10.** Ser transparente com o usuário e explicitar as medidas de segurança dos dados;
- 11.** Garantir a segurança dos dados por meio de ações periódicas de prevenção ao uso indevido dos mesmos;
- 12.** Informar o usuário caso aconteça um incidente de segurança.

ATUALIZE-SE



Por fim, o quanto antes os negócios se adequarem às novas normativas, melhor vai ser o processo de transição e menores serão os riscos de incorrerem em erro. As novas leis de proteção de dados trazem consigo desafios como a mudança de *mindset* do mercado e dos usuários. Se por um lado quem trabalhar com informações terá que se adequar às regras, por outro quem as fornece precisa entender que a autorização do uso de seus dados é crucial para uma publicidade mais direcionada e que realmente faça sentido. O segundo ponto pode ser feito por meio de educação de mercado estimulada pelas empresas.

Além disso, as companhias que trabalham com dados terão como desafio se adequar corretamente à legislação, manter uma fiscalização periódica para evitar erros e se expor quando sofrer incidentes de segurança, informando ao titular o acontecido e as providências tomadas para evitar novas falhas na segurança.

Cumpridas estas etapas, as empresas imprimem maior credibilidade ao seu negócio, demonstrando responsabilidade e compromisso com os seus usuários e parceiros. Além do mais, estar em conformidade com a lei é ter segurança jurídica, diminuindo os riscos de sanções e multas. As empresas que entrarem em *compliance* com as regras terão a seu favor também, vantagens competitivas frente aos concorrentes.



www.tail.digital

A Tail é uma plataforma de big data analytics, que oferece soluções para segmentação de campanha e gerenciamento de audiências através de uma [DMP](#). A plataforma de big data analytics da Tail também proporciona adequação e conformidade ao LGPD para quaisquer projetos de dados.

Clique no botão e acesse a nossa Central de Privacidade e confira mais informações.

Acesse agora